A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

PHILIP A. BLOOM; EBLOOM2357@HOTMAIL.COM : VERSION V

Abstract. An open problem is proving FLT *simply* (using Fermat's toolbox) for each $n \in \mathbb{N}, n > 2$. Our *direct proof* (not BWOC) of FLT is based on our algebraic identity $((r + 2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}} q)^n = ((r - 2q^n)^{\frac{1}{n}})^n$ with arbitrary values of $n \in \mathbb{N}$, and with $r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$. For convenience, we *denote* $(r+2q^n)^{\frac{1}{n}}$ by s; we *denote* $2^{\frac{2}{n}} q$ by t; and, we *denote* $(r-2q^n)^{\frac{1}{n}}$ by u. For any given $n > 2$: Since the term t or $2^{\frac{2}{n}} q$ with $q \in \mathbb{Q}$ is not rational, this identity allows us to relate null set $\{(s, t, u)|s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n\}$ with subsequently proven null set $\{z, y, x|z, y, x \in \mathbb{Q}, z, y, x > 0, z^n - y^n = x^n\}$: We show it is true, for $n > 0$, that $\{t|s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n\} = \{y|z, y, x \in \mathbb{Q}, z, y, x > 0, z^n - y^n = x^n\}$. Hence, for any given $n \in \mathbb{N}, n > 2$, it is a true statement that $\{(x, y, z)|x, y, z \in \mathbb{N}, x, y, z > 0, x^n + y^n = z^n\} = \varnothing$.

1. Introduction

FLT states : $x^n + y^n = z^n$ does not hold for $n > 2, n, x, y, z \in \mathbb{N}, x, y, z > 0$.

A *simple* (using Fermat's tools) proof of FLT for each $n \in \mathbb{N}, n > 2$ is lacking.

For $n \in \mathbb{N}, n > 2$: We propose a simple *direct proof* (not the expected BWOC).

(A) $z^n - y^n = x^n$, for $n > 0$, with $z, y, x \in \mathbb{Q}, z, y, x > 0$ for which (A) holds. We want an algebraic identity, with an irrational term for $n > 2$, to relate to (A).

(B) $((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}} q)^n = ((r-2q^n)^{\frac{1}{n}})^n$ for $n > 0, q \in \mathbb{Q}, r \in \mathbb{R}, n \in \mathbb{N}, q, r > 0$ such that $(r + 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}} q, (r - 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$ for which (B) holds. From an infinity of identities we choose (B). For values of $n > 2$: Equation (B) clearly does not hold for $(r + 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}} q, (r - 2q^n)^{\frac{1}{n}} \in \mathbb{Q}, q \in \mathbb{Q}, r \in \mathbb{R}$, but, (B) is consistent with (A) since for (z, y, x), no $z, y, z \in \mathbb{Q}$ is known for which (A) holds. Denoting $(r + 2q^n)^{\frac{1}{n}}$ by s; $2^{\frac{2}{n}} q$ by t; $(r - 2q^n)^{\frac{1}{n}}$ by u : We show, below, for $n > 2$, with both sets empty, that $\{(s, t, u)|s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z, y, x)|z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$

(C) $(r + q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}} q)^n = ((r - q^n)^{\frac{1}{n}})^n$: For relating to (A), a simpler such identity is (C), for $n > 0$, with $(r + q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}} q, (r - q^n)^{\frac{1}{n}} \in \mathbb{Q}, q \in \mathbb{Q}, r \in \mathbb{R}, q, r > 0$ for which (C) holds. But, for the values of $n = 2, q \in \mathbb{Q}$, equation (C) does not hold for $(r + q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}} q, (r - q^n)^{\frac{1}{n}} \in \mathbb{Q}$. So, (C) is *logically inconsistent with (A)*, making statement (C) a false premise from which nothing follows in our argument.

(D) $((r + 2^p q^n)^{\frac{1}{n}})^n - (2^{\frac{p+1}{n}} q)^n = ((r - 2^p q^n)^{\frac{1}{n}})^n$, for $n > 0$, with $n \in \mathbb{N}$, and $p \in \mathbb{I}, p \geq 0$, and $r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0$, and $(r + 2^p q^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}} q, (r - 2^p q^n)^{\frac{1}{n}} \in \mathbb{Q}$ for which the family of identities (D) holds. We have evaluated (D) for usefulness :

We reject (D) with even $p \geq 0, q \in \mathbb{Q}$ since, for $n = 2$, the middle part, $2^{\frac{p+1}{n}} q$, is not rational. We reject (D) with odd $p > 1, q \in \mathbb{Q}$ since for $2^{\frac{p+1}{n}} q \in \mathbb{Q}$, equation (B) yields the composite set of all elements contained in every set that (D) yields.

Date: February 18, 2019.

2. Our Direct Proof

Our argument is a *direct proof* without deriving a contradiction, as is generally expected. We start in the real realm, ending in the realm of natural numbers.

The algebraic identity we eventually relate to (A) $z^n - y^n = x^n$ is (1), below.

$$\left((r+2q^n)^{\frac{1}{n}}\right)^n - (2^{\frac{2}{n}}q)^n = \left((r-2q^n)^{\frac{1}{n}}\right)^n. \tag{1}$$

For all $n \in \mathbb{N}, n > 0$, identity (1) holds for *all* $r, q \in \mathbb{R}$ with $q, r > 0, r > 2q^n$.

(2) $((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})$ is the triple for which (1) holds, such that $(r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}$ with $r, q \in \mathbb{R}, r, q > 0$. We relate (2) with (3) :

(3) $z^n - y^n = x^n$. For some values of n, equation (3) holds for triple (z, y, x) such that $z, y, x \in \mathbb{R}, z, y, x > 0$. The set of n-th triples for which (3) holds is (4) :

(4) $\{z^n, y^n, x^n|, z, y, x \in \mathbb{R}, z, y, x > 0, z^n - y^n = x^n\}$.

Expanding each side of equation (1), above, yields equation (5), below :

(5) $(r+2q^n) - (4q^n) = r - 2q^n$. For some values of $n > 0$, equation (5) holds for $(r+2q^n, 4q^n, r-2q^n)$ such that $r+2q^n, 4q^n, r-2q^n \in \mathbb{R}, r, q \in \mathbb{R}$. Hence, per (5) :

(6) $\{(r+2q^n, 4q^n, r-2q^n)|r, q \in \mathbb{R}, (r+2q^n) - (4q^n) = r - 2q^n\}$ is the set of nth-triples for which (5) holds. Statement (7), below, is evidently true :

(7) $\{(r+2q^n, 4q^n, r-2q^n)|r, q \in \mathbb{R}, r, q > 0, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{z^n, y^n, x^n|z, y, x \in \mathbb{R}, z, y, x > 0, z^n - y^n = x^n\}$, since r, q are unrestricted real.

Taking a rational subset of each side of (7), such that $(r+2q^n, 4q^n, r-2q^n) \in \mathbb{Q}$, implying $q^n \in \mathbb{Q}$, thus, implying that $r \in \mathbb{Q}$, yields (8), below, with both subsets empty, or both subsets nonempty for $n > 0$:

(8) $\{(r+2q^n, 4q^n, r-2q^n)|r \in \mathbb{Q}, q \in \mathbb{R}, q^n \in \mathbb{Q}, (r+2q^n) - 4q^n = (r-2q^n)\} = \{z^n, y^n, x^n|z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$.

Taking a further rational subset, this time with each side of (8) yields (9), below, with both subsets empty, or both subsets nonempty for $n > 0$:

(9) $\{(r+2q^n, 4q^n, r-2q^n)|r \in \mathbb{Q}, q \in \mathbb{Q}, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{z^n, y^n, x^n|z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}$. Per (9) we get (10),(11),(12) for $n > 0$. :

(10) $\{r+2q^n|r+2q^n \in (9)\} = \{z^n|z^n \in (9)\}$ with both sets empty, or nonempty.

(11) $\{4q^n|4q^n \in (9)\} = \{y^n|y^n \in (9)\}$ with both sets empty, or both nonempty.

(12) $\{r-2q^n|r-2q^n \in (9)\} = \{z^n|z^n \in (9)\}$ with both sets empty, or nonempty.

(13) $r + 2q^n \in (10) = z^n \in (10)$.

(14) $4q^n \in (11) = y^n \in (11)$.

(15) $r - 2q^n \in (12) = x^n \in (12)$. Taking the n-th root of the values on each side of equations (13),(14),(15) yield, respectively, (16),(17),(18) for $n > 0$:

(16) $(r+2q^n)^{\frac{1}{n}} \in (B) = z \in (A)$.

(17) $(4q^n)^{\frac{1}{n}} \in (B) = y \in (A)$.

(18) $(r-2q^n)^{\frac{1}{n}} \in (B) = x \in (A)$. So, per (16),(17),(18), we determine the respective equations of sets (19),(20),(21), for each of which both sets are empty, or both sets are nonempty for $n > 0$:

(19) $\{(r+2q^n)^{\frac{1}{n}}|(r+2q^n)^{\frac{1}{n}} \in (B)\} = \{z|z \in (A)\}$.

(20) $\{(4q^n)^{\frac{1}{n}}|(4q^n)^{\frac{1}{n}} \in (B)\} = \{y|y \in (A)\}$.

(21) $\{(r-2q^n)^{\frac{1}{n}}|(r-2q^n)^{\frac{1}{n}} \in (B)\} = \{x|x \in (A)\}$. Therefore, per (19),(20),(21):

(22) $\{((r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}})|(r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}} \in \mathbb{Q}, r \in \mathbb{Q}, q \in \mathbb{Q}, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{(z, y, x)|z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}$, for any given $n \in \mathbb{Q}, n > 0$, with both sets empty or both sets nonempty.

3. Results and Conclusion

Consequently, per (22) solely $q \in \mathbb{Q}$ is sufficient in our argument.

In this section, for convenience only :
(23) *Let* $(r + 2q^n)^{\frac{1}{n}}$ in (B) be s; *let* $2^{\frac{2}{n}}q$ in (B) be t; *let* $(r - 2q^n)^{\frac{1}{n}}$ in (B) be u.

(24) $\{(s,t,u)|s,t,u \in (B)\} = \{(z,y,x)|z,y,x \in (A)\}$ per (22),(23), above.

Taking the integral subset of values on each side of (24) results in (25), below :
(25) $\{(s,t,u)|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

Some concrete examples of (25) : For $n = 2$, with $z = 5, y = 4, x = 3$ in (A), there is a corresponding $s = 5, t = 4, u = 3$ in (B) resulting from r in (B) $= \frac{41}{2}$ and q in (B)$= \frac{3}{2}$. For $n = 1$, with $z = 13, y = 12, x = 1$ in (A), there is a corresponding $s = 13, t = 12, u = 1$ in (B) resulting from r in (B) $= \frac{25}{2}$ and q in (B) $= \frac{1}{4}$.

(26) $\{t|t \in \mathbb{Q}, s,u \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n\} = \varnothing$ for $n > 2$, which is true since t is $2^{\frac{2}{n}}q$, per (23), so, $2^{\frac{2}{n}}q$ is irrational with $q \in \mathbb{Q}$. Hence, per (25),(26) :
(27) $\{y|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$. Thus, per (A) :
(28) $\{(z,y,x)|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$. So, per (28):
(29) $x^n + y^n = z^n$, for $n \in \mathbb{N}, n > 2$, does not hold for $x,y,z \in \mathbb{N}, x,y,z > 0$.

(30) QED.